(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 42 43 908 A 1**

(51) Int. Cl.[5]:
H 04 L 9/32
H 04 L 9/30

(21) Aktenzeichen: P 42 43 908.6
(22) Anmeldetag: 23. 12. 92
(43) Offenlegungstag: 30. 6. 94

DE 42 43 908 A 1

(71) Anmelder:
GAO Gesellschaft für Automation und Organisation mbH, 81369 München, DE

(74) Vertreter:
Klunker, H., Dipl.-Ing. Dr.rer.nat.; Schmitt-Nilson, G., Dipl.-Ing. Dr.-Ing.; Hirsch, P., Dipl.-Ing., Pat.-Anwälte, 80797 München

(72) Erfinder:
Albert, Bodo, 8000 München, DE

(54) Verfahren zur Erzeugung einer digitalen Signatur mit Hilfe eines biometrischen Merkmals

(57) Es wird ein Verfahren zur Erzeugung einer digitalen Signatur vorgestellt, in dem der geheime Schlüssel bei jeder Erzeugung mittels eines biometrischen Merkmals generiert wird. Dazu wird das biometrische Merkmal benutzerspezifisch in einen digitalen, individuellen Wert übergeführt. Dieser Wert ist reproduzierbar und dient als Ausgangswert für die Berechnung des geheimen Schlüssels.

DE 42 43 908 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 05. 94 408 026/164

Beschreibung

Die Erfindung betrifft ein Verfahren zur Erzeugung einer digitalen Signatur gemäß dem Oberbegriff des Anspruchs 1.

Signaturen dienen im allgemeinen der Unterzeichnung von Texten, so daß diese ihrem Verfasser eindeutig zugeordnet werden können. Mit der ständig wachsenden Automatisierung im Austausch von Nachrichten in Computersystemen entsteht auch hier ein natürliches Bedürfnis, diese Nachrichten eindeutig ihrem Verfasser zuordnen zu können. Aus diesem Grunde versieht man die digitalisierten Nachrichten mit einer digitalen Signatur, die ähnliche Eigenschaften, wie die aus dem Schriftverkehr bekannte Signatur (Unterschrift), aufweist. Insbesondere muß sichergestellt sein, daß nur eine einzige Person eine von ihr verfaßte Nachricht mit der eigenen digitalen Signatur versehen kann. Von gleicher Wichtigkeit ist die einfache, eindeutige Zuordnung der digitalisierten Signatur zum Unterzeichner. Dies muß auch dann noch möglich sein, wenn zwischen der Unterzeichnung der Nachricht und der Prüfung der Authentität der Unterschrift schon eine geraume Zeit vergangen ist. Schließlich muß die Signatur in einer Art und Weise erstellt werden, die garantiert, daß ihr Erzeuger seine eigene Unterschrift nicht verleugnen kann.

Verfahrensarten zur Erstellung der digitalen Signatur, welche die o.g. zur Sicherheit notwendigen Eigenschaften gewährleisten, sind asymmetrische Signaturverfahren. In solchen Verfahren werden jedem möglichen Sender von Nachrichten ein geheimer und ein öffentlicher Schlüssel zugeordnet, so daß jeder Sender ein ihm eigenes Schlüsselpaar besitzt.

Mit dem geheimen Schlüssel eines Benutzers wird eine digitalisierte Nachricht in eine Zeichenfolge transformiert. Das Ergebnis dieser Transformation ist die Signatur. Gegebenenfalls kann die Nachricht vor der Transformation komprimiert werden, was im allgemeinen die Durchführung der Transformation beschleunigt und zu immer gleichlangen Signaturen führt.

Die digitalisierte Nachricht und die Signatur werden von dem Sender an den Empfänger übermittelt. Dieser komprimiert die empfangene Nachricht genauso wie der Sender und wendet auf die Signatur eine Rücktransformation mit dem öffentlichen Schlüssel des Senders an. Hierbei kennt der Empfänger die Zuordnung des öffentlichen Schlüssels zum Sender, so daß er bei der Rücktransformation den richtigen öffentlichen Schlüssel verwenden kann. Die Authentizität der Nachricht ist genau dann erwiesen, wenn die vom Empfänger komprimierte Nachricht mit der Zeichenfolge übereinstimmt, die aus der Rücktransformation der Signatur entsteht.

Die oben verwendete Bezeichnung "digitale Signatur" ist deswegen gerechtfertigt, weil ausschließlich diejenige Person ihre eigene Signatur erzeugen kann, die im Besitz des Geheimschlüssels ist. Die Rücktransformation der Signatur und damit ihre Verifizierung kann hingegen mit Hilfe des öffentlichen Schlüssels von jeder Person durchgeführt werden. Diese Eigenschaften sind aufgrund der Asymmetrie des Verfahrens gewährleistet, da hier die Möglichkeit der Rücktransformation nicht auch automatisch zur Transformation und damit zur Erzeugung von echten Signaturen befähigt.

Die Sicherheit des oben vorgestellten Systems ist unmittelbar davon abhängig, wie schwierig es für Dritte ist, unrechtmäßig zu der Kenntnis des geheimen Schlüssels einer Person zu kommen. Gelangt nämlich beispielsweise ein Betrüger in den Besitz des geheimen Schlüssels einer Person, so ist er in der Lage, ihre Signatur zu erzeugen und sich ihre Identität anzueignen. Der geheime Schlüssel ist also besonders gut vor unrechtmäßigem Zugang zu schützen.

Zur Realisierung dieses Schutzes wird z. B. in dem Artikel "Public key versus conventional key encryption" aus National computer conference 1979 vorgeschlagen, den geheimen Schlüssel an einem sicheren Ort zu speichern. Der einem Systembenutzer zugeordnete geheime Schlüssel wird nur dann freigegeben, wenn der Benutzer seine Identität eindeutig nachgewiesen hat. Der geheime Schlüssel wird entweder in einer dem Benutzer gehörenden Medium (beispielsweise eine IC-Karte) oder aber im System selbst gespeichert.

Befindet sich der Speicher auf einem tragbaren Medium, so besteht die Gefahr, daß es verloren oder vergessen wird und im Bedarfsfall nicht zur Verfügung steht.

Bei der Speicherung der geheimen Schlüssel aller Systembenutzer im System selbst ist dort ein Speicher mit ausreichender Speicherkapazität zur Verfügung zu stellen.

In beiden Fällen ist jedenfalls ein Ausspähen des Schlüssels, da dieser immer existent ist, denkbar, wodurch die Sicherheit des Systems gefährdet ist.

Der Erfindung liegt somit die Aufgabe zugrunde, ein Verfahren zur Erzeugung einer digitalen Signatur vorzustellen, bei dem das Ausspähen des Schlüssels über das bekannte Maß hinaus erschwert wird.

Die Aufgabe wird durch die im kennzeichnenden Teil des Hauptanspruchs angegebenen Merkmale gelöst.

Der Grundgedanke der Erfindung besteht darin, auf einen zusätzlichen Speicher als Träger des geheimen Schlüssels zu verzichten und den geheimen Schlüssel erst in dem Moment zu generieren, in dem er gebraucht wird.

Ausgangspunkt für die Bildung des geheimen Schlüssels ist ein biometrisches Merkmal, wie z. B. ein Fingerabdruck, die Handgeometrie, die Stimme etc., wobei in einem System immer das gleiche Merkmal, beispielsweise der Fingerabdruck verwendet wird. Aus diesem Merkmal wird indirekt der geheime Schlüssel berechnet. Hierbei ist sicherzustellen, daß die Berechnung des Schlüssels immer zu dem gleichen Ergebnis führt, um eindeutige Signaturen erzeugen zu können. Dazu bildet man bei jeder Anwendung des Verfahrens aus dem biometrischen Merkmal einen digitalen Wert zur Berechnung des Schlüssels. Dieser digitale Wert wird in einen individuellen Wert überführt, der in einer eindeutigen Beziehung zu dem biometrischen Merkmal steht. Die Überführung des digitalisierten Wertes in den individuellen Wert wird reproduzierbar vorgenommen, so daß bei jeder Anwendung des Systems durch einen Benutzer der gleiche individuelle Wert erstellt wird. Der individuelle Wert wird nun als Ausgangswert zur Berechnung des geheimen Schlüssels verwendet, was wegen der Reproduzierbarkeit des individuellen Wertes immer zum gleichen Ergebnis führt. Nachdem der geheime Schlüssel berechnet ist, erfolgt die Erstellung der Signatur in der üblichen Art und Weise.

Die mit der Erfindung erzielten Vorteile bestehen insbesondere darin, daß weder der geheime Schlüssel selbst noch geheime Ausgangswerte zur Bildung des geheimen Schlüssels im System permanent gespeichert sind. Es ist also einerseits kein Speichermedium erforderlich, welches der Person zugeordnet ist (z. B. IC-Karte), andererseits braucht im System kein Speicher mit einer genügend großen Speicherkapazität zur Speiche-

rung aller geheimen Schlüssel bzw. geheimen Ausgangswerte zur Berechnung der geheimen Schlüssel zur Verfügung gestellt werden. Da der geheime Schlüssel erfindungsgemäß weder langfristig noch kurzfristig in einem separaten Speicher abgelegt ist, kann auf Maßnahmen, z. B. kryptografischer Art, verzichtet werden, um einen langfristig in einem separaten Speicher abgelegten Schlüssel vor Ausspähung zu schützen. Der geheime Schlüssel ist jeweils nur zur Erzeugung der Unterschrift temporär im System gespeichert.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Zeichnung.

Darin zeigt:

Fig. 1 ein Blockschaltbild eines Systems zur Erzeugung digitaler Signaturen,

Fig. 2 den Teil des Blockschaltbildes aus Fig. 1, in dem der Schlüssel generiert wird.

Digitale Signaturen können mit Hilfe sogenannter Public Key-Verfahren erzeugt werden. Die nun folgende Beschreibung basiert auf der Erzeugung digitaler Signaturen durch den RSA-Algorithmus, der allerdings nur beispielhaft gewählt ist. Die Berechnung der im RSA-Algorithmus verwendeten Schlüssel eines Benutzers gründet im wesentlichen auf der Auffindung zweier Primzahlen p und q. Diese Primzahlen sind geheimzuhalten, da mit ihr-er Kenntnis Rückschlüsse auf den einem Benutzer zugeordneten geheimen Schlüssel zu ziehen sind. Im folgenden wird lediglich die erfindungsgemäße Erzeugung des geheimen Schlüssels in RSA-System erläutert und auf die sonstigen Verfahrensschritte nur am Rande eingegangen. Auf eine genaue Erläuterung des RSA-Algorithmus selbst wird verzichtet, es sei aber schon an dieser Stelle auf die zum RSA-Algorithmus bekannt gewordene einschlägige Literatur hingewiesen.

Fig. 1 zeigt anhand eines Blockschaltbildes ein System zur Bildung digitaler Signaturen gemäß der Erfindung. In einem Analogmeßteil 1 wird zunächst ein biometrisches Merkmal des Senders A einer Nachricht erfaßt. Dies führt zu einem Meßwert, der als analoges biometrisches Merkmal (ABM) bezeichnet ist. Das analoge biometrische Merkmal wird in einem Analog/Digitalwandler 2 in ein digitales biometrisches Merkmal (DBM) 3 umgewandelt.

Das digitale biometrische Merkmal 3 wird an die Systemkomponente 5 übermittelt. Dort wird in dem Schlüsselgenerator 6 der geheime Schlüssel SK(A) des Senders A berechnet (siehe auch Beschreibung zu Fig. 2). Der Index A in SK(A) weist darauf hin, daß dieser geheime Schlüssel eindeutig dem Sender A zugeordnet ist. Diese Schreibweise wird auch für andere Schlüssel beibehalten.

Der geheime Schlüssel SK(A) wird in eine Einrichtung 9 gegeben. Auf einen zweiten Eingang der Einrichtung 9 wird der zu übermittelnde Text T bzw. die Zeichenfolge T' gegeben und mit dem geheimen Schlüssel SK(A) transformiert.

Die Zeichenfolge T' entsteht beispielsweise durch die Anwendung einer Hashfunktion auf den Text T, die ihn komprimiert. Diese Komprimierung ist nicht zwingend notwendig, beschleunigt aber im allgemeinen die Transformation und erzeugt unabhängig von der Länge des Textes T immer eine gleichlange Zeichenfolge T'.

Das Ergebnis der Transformation mit dem dem Sender A eindeutig zugeordnetem geheimen Schlüssel ist die Signatur S. Im Falle der Komprimierung weist die Signatur S bei jeder Unterzeichnung die gleiche Länge auf.

Die Signatur S, der Text T und gegebenenfalls der öffentliche Schlüssel PK(A) des Senders A werden an den Empfänger 13 übermittelt. Dieser wendet auf die Signatur S mit dem öffentlichen Schlüssel SK(A) eine Rücktransformation an, was auf die Zeichenfolge T* führt. Ferner wird der übermittelte Text T durch die Hashfunktion h in die Zeichenfolge T' transformiert. In dem Vergleicher 15 werden die Zeichenfolgen T* und T' miteinander verglichen. Bei Gleichheit ist die Authentität des Textes T und die Echtheit der Signatur des Senders A erwiesen.

Es sei bemerkt, daß der öffentliche Schlüssel PK(A) nicht von der Systemkomponente 5 an den Empfänger 13 übermittelt zu werden braucht, sondern vielmehr auch bei diesem gespeichert sein kann.

Fig. 2 zeigt den Schlüsselgenerator 6 der Systemkomponente 5 im Detail. In dem Schlüsselgenerator 6 wird bei jeder Anwendung des Systems bzw. bei jeder Erstellung einer digitalen Signatur durch einen Sender der geheime und der öffentliche Schlüssel des Senders neu berechnet. Diese Berechnung benutzt das digitalisierte biometrische Merkmal 3 des Senders als Ausgangswert, wobei bei der Berechnung nicht auf im System gespeicherte, geheime Werte zurückgegriffen wird.

Zunächst wird zur Berechnung des Schlüssels auf das in den Schlüsselgenerator 6 eingespeiste digitale biometrische Merkmal 3 die Funktion f angewendet, die dem Merkmal einen individuellen Wert IW zuordnet.

Die mathematische Funktion f ist dabei so zu wählen, daß eventuelle Toleranzen, welche beim analogen Messen des biometrischen Merkmals des Benutzers auftreten können und sich somit auf das digitalisierte biometrische Merkmal 3 auswirken, bei der Berechnung des individuellen Wertes IW des Benutzers herausgefiltert werden. Dies kann beispielsweise dadurch geschehen, daß nur diejenigen Binärstellen des digitalisierten biometrischen Merkmals 3 zur Berechnung des individuellen Wertes IW beitragen, die sich als stabil, d. h. unveränderlich, erweisen. Dadurch ist gewährleistet, daß bei jeder Benutzung des Systems die Anwendung der Funktion f auf das digitalisierte biometrische Merkmal 3 eines Benutzers auf den gleichen individuellen Wert IW führt und dieser somit reproduzierbar ist.

Neben der Eigenschaft der Herausfilterung von Fehlern bei der Messung des biometrischen Merkmals ist die mathematische Funktion f so auszulegen, daß den digitalisierten biometrischen Merkmalen 3 zweier willkürlich ausgewählter Systembenutzer zwei unterschiedliche individuelle Werte IW zugeordnet werden. Mit anderen Worten: die Funktion f sollte für jeden Benutzer einen individuellen Wert erzeugen. Bei einer sehr großen Anzahl von Benutzern darf die Funktion f zwei Systembenutzern den gleichen individuellen Wert IW nur mit einer so geringen Wahrscheinlichkeit zuordnen, daß dies mit der Sicherheit des Systems zu vereinbaren ist.

Aus den obigen Betrachtungen wird deutlich, daß die Funktion f einem digitalisierten biometrischen Merkmal 3 und damit einem Benutzer bei jeder Messung einen individuellen, reproduzierbaren Wert IW zuordnen muß.

Der mit Hilfe der Funktion f aufgefundene individuelle Wert IW wird zur Berechnung des geheimen Schlüssels des Systembenutzers weiterverwendet.

Dazu wird die Funktion f so gewählt, daß die individuellen Werte IW aller Systembenutzer die gleiche Länge

von z. B. 1024 Bit aufweisen. Aus dieser 1024 Bit langen Zeichenfolge Z eines Benutzers werden beispielsweise zwei gleich lange Zeichenfolgen Z(1) und Z(2) gebildet, die jeweils 512 Bit lang sind. Hierbei wird die erste Zeichenfolge Z(1) durch die ersten 512 Bit und die zweite Zeichenfolge Z(2) durch die letzten 512 Bit des individuellen Wertes IW dargestellt.

Jede der beiden Zeichenfolgen Z(1) und Z(2) wird als binärcodierte natürliche Zahl interpretiert, die man zur Bestimmung der Primzahlen p bzw. q heranzieht. Dabei kann die Primzahl p in dem Rechner 25 z. B. dadurch eindeutig festgelegt werden, daß man, ausgehend von der natürlichen Zahl Z(1), auf dem Zahlenstrahl der natürlichen Zahlen die nächste Primzahl sucht, die großer als die Zahl Z(1) ist. In analoger Art und Weise läßt sich ausgehend von der natürlichen Zahl Z(2) die zweite Primzahl q eindeutig berechnen.

Es sei an dieser Stelle erwähnt, daß der oben erläuterte Weg zur Berechnung der Primzahlen p und q nur beispielhaft gewählt ist. Andere Wege zur Bestimmung sind denkbar. Wichtig ist lediglich, daß durch einen bestimmten Systembenutzer bei jeder Anwendung des Systems die gleichen Primzahlen p und q generiert werden. Nur dann kann bei jeder Anwendung der richtige geheime Schlüssel eines Benutzers berechnet und eine echte, dem Benutzer zugeordnete digitale Signatur erzeugt werden. In dem oben erläuterten Beispiel ist die eindeutige Berechnung der Primzahlen durch die Reproduzierbarkeit des individuellen Wertes IW gewährleistet, der als Startwert zur Bestimmung von p und q dient.

Es ist der einschlägigen Fachliteratur zu entnehmen, daß die Angabe eines bestimmten Primzahlenpaares p und q im RSA-Algorithmus allein nicht ausreichend ist, um den geheimen und öffentlichen Schlüssel eines Benutzers eindeutig festzulegen. Zu dieser Festlegung bedarf es vielmehr noch zusätzlicher Parameter, die entweder fest vorgegeben sind oder aber reproduzierbar aus dem individuellen Wert IW abgeleitet werden.

In Computersystemen, in denen digitale Signaturen erzeugt werden, werden nichtgeheime Daten, insbesondere die öffentliche Schlüssel der Systembenutzer, häufig im System gespeichert. Diese Speicherung des öffentlichen Schlüssels in Verbindung mit der Identität des Benutzers kann z. B. bei einer übergeordneten, vertrauenswürdigen Instanz stattfinden. Unter Einbezug dieser Instanz in den Datenaustausch kann dann sichergestellt werden, daß nur zugelassene öffentliche Schlüssel verwendet werden und es einem Systembenutzer praktisch nicht mehr möglich ist, seinen öffentlichen Schlüssel unter einem falschen Namen bekanntzumachen und sich somit eine falsche Identität anzueignen. Die Verfahren zur Zertifizierung im System zugelassener Schlüssel sind aus der einschlägigen Literatur bekannt, so daß darauf nicht näher eingegangen werden soll.

Patentansprüche

1. Verfahren zur Erzeugung einer digitalen Signatur durch die Digitalisierung und gegebenenfalls Komprimierung eines Klartextes und die Transformation des digitalisierten, komprimierten Textes mit einem geheimen, einem Benutzer zugeordneten Schlüssel, **dadurch gekennzeichnet**, daß zu jeder Erzeugung der digitalen Signatur gegebenenfalls neben anderen Daten auch ein biometrisches Merkmal des Benutzers meßtechnisch erfaßt und als Ausgangswert zur Erzeugung des geheimen Schlüssels mit herangezogen wird.

2. Verfahren zur Erzeugung einer digitalen Signatur nach Anspruch 1, dadurch gekennzeichnet, daß das biometrische Merkmal analog erfaßt und das so erhaltene analoge biometrische Merkmal in ein digitalisiertes biometrisches Merkmal umgewandelt und aus dem digitalisierten biometrischen Merkmal der geheime Schlüssel generiert wird.

3. Verfahren zur Erzeugung einer digitalen Signatur nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß das digitalisierte biometrische Merkmal in einen individuellen Wert übergeführt wird, der dem Inhaber des biometrischen Merkmals eindeutig zugeordnet ist und die Überführung des digitalisierten biometrischen Merkmals in den individuellen Wert bei jeder Generierung des geheimen Schlüssels in dem gleichen individuellen Wert resultiert.

4. Verfahren zur Erzeugung einer digitalen Signatur nach Anspruch 1, dadurch gekennzeichnet, daß zur Transformation ein Public Key-Verfahren eingesetzt wird.

5. Verfahren zur Erzeugung einer digitalen Signatur nach Anspruch 4, dadurch gekennzeichnet, daß der RSA-Algorithmus verwendet wird und die in den RSA-Algorithmus zur Bestimmung des geheimen Schlüssels einfließenden Primzahlen p und q aus dem individuellen Wert berechnet werden.

6. Verfahren zur Erzeugung einer digitalen Signatur nach Anspruch 5, dadurch gekennzeichnet, daß die Länge des individuellen Wertes für alle Benutzer gleich ist und aus einem ersten Teil dieser digitalisierten Zeichenfolge die Primzahl p und aus einem zweiten Teil die Primzahl q bestimmt wird.

7. Verfahren zur Erzeugung einer digitalen Signatur nach Anspruch 6, dadurch gekennzeichnet, daß jede der beiden Teile der Zeichenfolge des individuellen Wertes als binärcodierte natürliche Zahl aufgefaßt wird und die jeweilige Primzahl p bzw. q dadurch festgelegt wird, daß man ausgehend von dieser natürlichen Zahl die nächste Primzahl sucht, die größer als die vorgegebene natürliche Zahl ist.

8. Vorrichtung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Vorrichtung

- ein Analogmeßteil zur Erfassung eines biometrischen Merkmals,
- einen Analog/Digitalwandler zur Umwandlung des analog erfaßten biometrischen Merkmals in ein digitalisiertes biometrisches Merkmal und
- einen Schlüsselgenerator zur Generierung des geheimen Schlüssels aus dem digitalisierten biometrischen Merkmal aufweist.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 42 43 908 A1
Int. Cl.[5]: H 04 L 9/32
Offenlegungstag: 30. Juni 1994

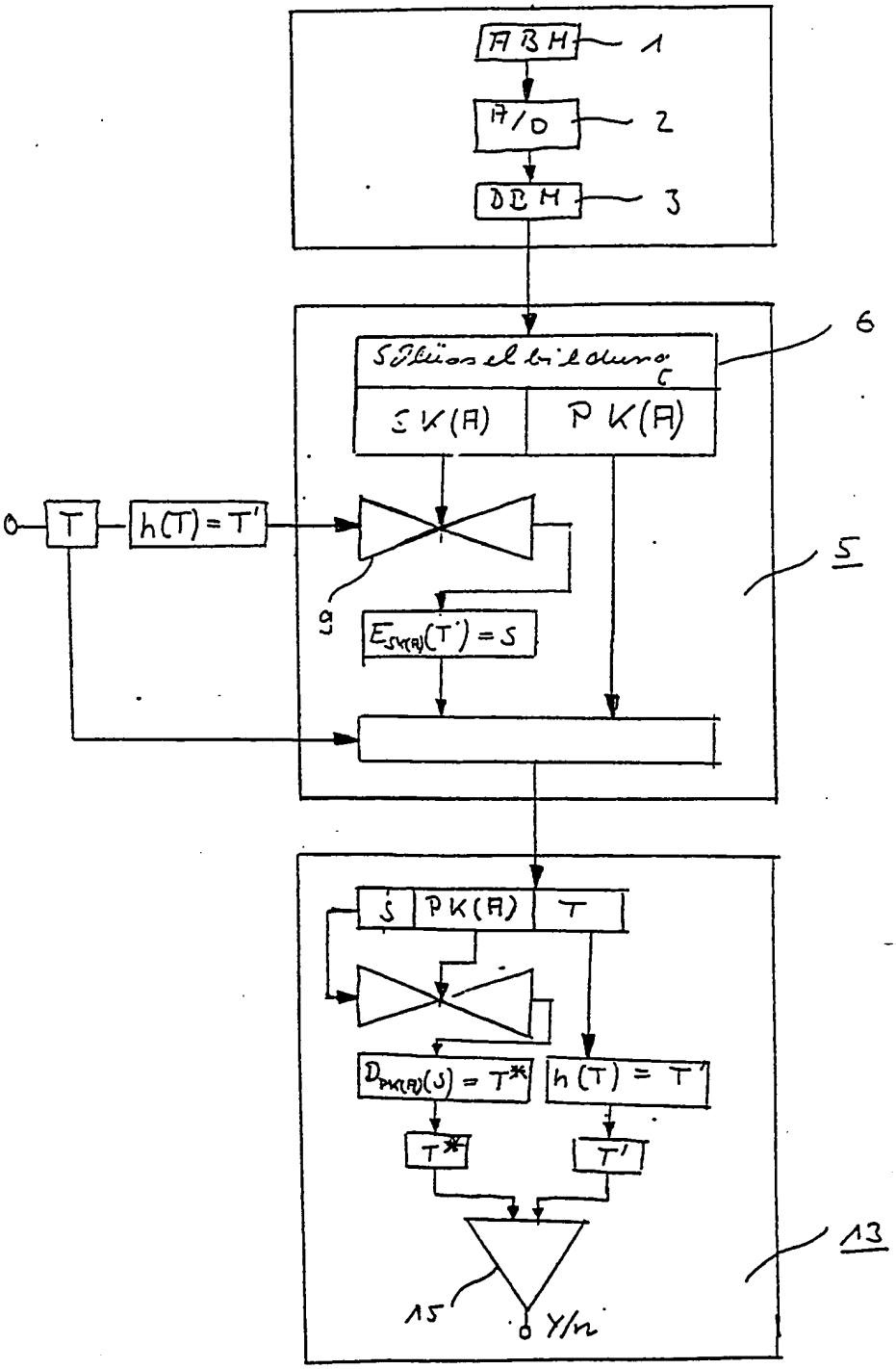

Fig. 1

Nummer: DE 42 43 908 A1
Int. Cl.[5]: H 04 L 9/32
Offenlegungstag: 30. Juni 1994

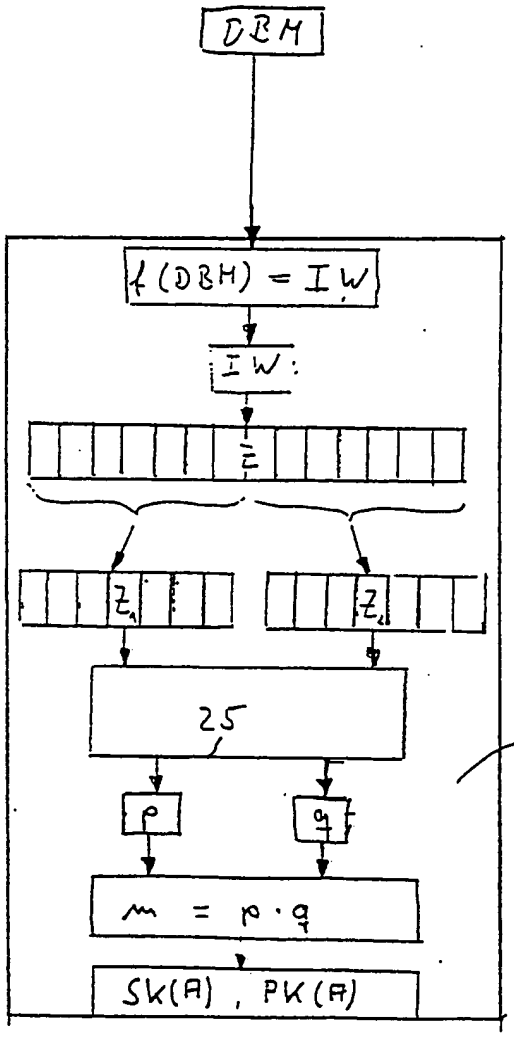

Fig. 2